UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,131	10/23/2003	Jae Doo Huh	5895P044	1681

8791 7590 01/27/2009

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
01/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/693,131	HUH ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 November 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24 and 29-35* is/are pending in the application.

4a) Of the above claim(s) *29-35* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 10/23/2003; amendment filed 11/6/2008.

2. Claims 1-24 are pending in the case.

Response to Arguments

3. Response to applicant's arguments is as follows:

4. Rejection under section 112, first paragraph:

The rejection is withdrawn due to amendments by the applicant.

5. Rejection under section 103:

Applicant argues that Examiner's Official Notice, stating that inclusion of an additional data field in a message to include additional information is known in the art is unsupported. Examiner hereby refers to US Patent Application 2003/0147534 to Ablay et al, at paragraph [0040], where a message includes several fields. The Public Key field is considered optional. Therefore, Ablay teaches a message consisting of several

fields, some of which are optional. This teaches a message including optional additional data fields to include additional information. This example is particularly relevant because the optional fields is actually a field containing the public key.

As another example, see US Patent No. 6105012 to Chang, at Fig. 7 and associated text, indicating a registration message including a field containing the public key. US 2004/0255037 to Corvari et al, at paragraph [0042] present another example. Therefore, applicant's argument is non persuasive.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 1 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Security Model and Authentication Protocol in EPON-based Optical Access Network, (hereinafter called Roh) by Roh and Kim, published as part of Transport Optical Networks, 2003, Proceedings of the 2003 5th International Conference on 29 June-3 July 2003 (volume 1), in view of Examiner's Official Notice, and further in view of

"PGP Message Exchange Formats; Request for Comments (RFC) 1991, by D. Atkins, W. Stallings, and P Zimmerman, dated August 1996, hereinafter called Atk."

7.1. As per claim 1, Roh is directed to a key management device for provision of a security service in an Ethernet-based passive optical network (abstract), comprising: an optical line terminal for sending a discovery gate message to discover an optical network unit for data transmission (Fig. 3 and associated text, where GATE(Discover Gate) is sent from the OLT to ONU), the discovery message including a public key of the optical line terminal (as shown in Roh Fig. 3, the OLT sends its public key to the ONU, but it does not explicitly show that the key is included in the discovery message. Examiner takes the Official Notice that inclusion of an extra field in a message to include additional information was well-known in the art at the time of invention. Therefore, it would have been obvious to add the public key to the gate discovery message. This is because Roh shows that the public key is to be sent via a message. One with ordinary skills in art would be motivated to include the public key in the gate discovery message because it will allow a reduction of number of message exchanged during the secured registration process), and, if said optical network unit receives said discovery gate message and then requests data communication (Fig. 3, the REGISTER REQUEST message), sending an encrypted registration message including a permanent medium access control (MAC) address of said optical network unit to said optical network unit to notify said optical network unit that it has been registered and a general gate message encrypted by a session key, including said permanent MAC

address of said optical network unit to said optical network unit to allocate a time slot to said optical network unit (Fig. 3, the REGISTER message, along with the GATE(GRANT), and the key certification. Note that the system is based on the Ethernet protocol, and therefore each message exchanged between communicating entities contains the MAC address. Also note that Roh teaches that after the session key is established between the ONU and OUT, all control messages and data messages are encrypted using the session key);

and said optical network unit for receiving said discovery gate message and then sending a registration request message, including said session key that is encrypted by said public key, with said session key encrypting all fields of the registration request message except for said session key that is encrypted by said public key, to said optical line terminal to request the data communication therewith and a registration acknowledgement message, encrypted by said session key to said optical line terminal to respond to said registration message (Fig. 3, the responses from the ONU to OLT corresponding to messages sent from OLT to ONU. Note that Roh also teaches sending the session key encrypted by OLT's public key to the OLT. Therefore both Roh and the claimed invention establish the session key at the OLT by sending the session key encrypted by the public key. Roh discloses sending a registration message. Roh also discloses using the session key for secured communication between the ONU and OLT as soon as the session key is established. However, Roh does not explicitly teach a message with all fields encrypted with a session key, except for the session key

being encrypted with a public key. Atk section 2.2 teaches a message encrypted with a session key, including the session key, which is encrypted with receiver's public key.

Roh and Atk are analogous art, as they are both directed to secured data transmission in networks. At the time of invention, it would have been obvious to the one skilled in the art to combine the messages sent between OLT and ONU in Roh into one message including the session key encrypted with receiver's public key, and other fields encrypted with the session key. The motivation would have been to improve the security of the transmissions by using a session key only once as indicated in Atk.

7.2. Limitations of claim 14 are substantially the same a claim 1.

8. Claims 2-13, and 15-24 rejected under 35 U.S.C. 103(a) as being unpatentable over Roh and Atk in view of Examiner's Official Notice as applied to claim1 above, and further in view of Cryptography and Network Security, by W. Stallings, 2nd Edition, 1999, hereinafter called Stallings.

8.1. As per claim 3, Roh is directed to the key management device as set forth in claim 1, wherein said discovery gate message includes a time slot field allocated to said optical network unit for registration thereof, a capability of said optical line terminal, a public key of said optical line terminal, and a nonce encrypted by a private key of said optical line terminal for signature (Based on Roh section 4.1, after the session key is

exchanged between OLT and ONU, all communications are encrypted for security using the session key. However, Roh does not specifically describe use of a private key system and a signature to enhance the security of communication.

Stallings teaches use of private key systems and signature to protect data communication. Stallings also teaches details of key exchange protocols to exchange the private/public keys and signature keys, when a session key is established between parties.

At the time of invention, it would have been obvious to the one skilled in art, to enhance the security of the system taught by Roh, by using private key protocols and digital signatures as taught by Stallings.

The motivation to do so would have been to improve the system security. Note that Roh section 4.2. identifies Stallings as a reference for teaching encryption protocols to enhance security.

All the fields, such as the time slot field, are part of EPON protocol).

8.2. As per claim 2, Roh is directed to the key management device as set forth in claim 1, wherein said discovery gate message is periodically sent (per Ethernet

protocol, discovery messages are periodically sent from OLT to discover new elements seeking to connect).

8.3. As per claim 4, Roh is directed to the key management device as set forth in claim 1, wherein said registration request message includes a physical ID capability, a capability of said optical network unit, an echo of a capability of said optical line terminal, a session key, a nonce decrypted by a public key of said optical line terminal, and a nonce created for signature of said optical network unit (Examiner take the official notice that all the exchanged fields are well known as part of EPON protocol, and therefore, would have been obvious to include in the security protocol taught by Roh).

8.4. As per claim 5, Roh is directed to the key management device as set forth in claim 4, wherein said physical ID capability, said capability of said optical network unit, said echo of said capability of said optical line terminal, said nonce decrypted by said public key of said optical line terminal and said nonce created for the signature of said optical network unit are encrypted using said session key (see response to claim 4).

8.5. As per claim 6, Roh is directed to the key management device as set forth in claim 4, wherein said session key is encrypted using said public key of said optical line terminal (see response to claim 4 and 1).

8.6. As per claim 7, Roh is directed to the key management device as set forth in claim 1, wherein said registration message further includes a physical ID list, an echo of a capability of said optical network unit, and a signature of said optical network unit (see response to claim 4).

8.7. As per claim 8, Roh is directed to the key management device as set forth in claim 1, wherein said general gate message further includes a time slot field for upstream transmission of said optical network unit (see response to claim 4).

8.8. As per claim 9, Roh is directed to the key management device as set forth in claim 8, wherein said general gate message is encrypted using a session key (see response to claims 1 and 4).

8.9. As per claim 10, Roh is directed to the key management device as set forth in claim 1, wherein said registration acknowledgement message includes a session key encrypted by a public key of said optical line terminal, and an echo of a registered physical ID (see response to claims 1 and 4).

8.10. As per claim 11, Roh is directed to the key management device as set forth in claim 10, wherein said registration acknowledgement message is encrypted using said session key (see response to claims 1 and 4).

8.11. As per claim 12, Roh is directed to the key management device as set forth in claim 1, wherein said optical line terminal includes: a public key processor for creating a public key to be included in said discovery gate message, and encrypting and decrypting said public key; a session key processor for decrypting said registration request message and registration acknowledgement message from said optical network unit using a session key, and encrypting said general gate message and registration message using said session key; a private key processor for creating a private key using said public key for encryption of messages to be transmitted to said optical network unit and decryption of messages received from said optical network unit, and encrypting and decrypting said private key; and storage means for storing and managing said public key, session key and private key (All the processes in the claim are addressed in claims 1-11 above. Once the processes are taught, the hardware (processor) to perform said processes in the OLU and ONT is also taught, as it is a trivial requirement to develop the system).

8.12. As per claim 13, Roh is directed to the key management device as set forth in claim 1, wherein said optical network unit includes: a session key processor for creating a session key for encrypted communication with said optical line terminal, encrypting a part of said registration request message using said session key, decrypting said registration message and general gate message from said optical line terminal using said session key and encrypting said registration acknowledgement message using said session key; a public key processor for encrypting said session key using a public key

from said optical line terminal; and storage means for storing said session key and public key (see response to claim 12. Note that performing decryption to access encrypted data is an integral part of encryption systems taught by Stallings).

8.13. Limitations of claims 15-24 are substantially the same as claims 2-13 above.

8.14. Claims 29-35 are withdrawn from consideration by the applicant's election in response to restriction requirement. Claims 25-28 are cancelled.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

1/20/2009

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434